

Exhibit B

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
SAN ANTONIO

F & J SAMAME, INC.
Plaintiff

v.

CIV. ACTION NO. 5:13-cv-00365-XR

ARCO IRIS ICE CREAM, ET AL.
Defendants.

Report of Computer Forensic Examination

Scope and Sources

On May 27, 2014, Judge Xavier Rodriguez appointed me to serve as Special Master for Electronically Stored Information ("ESI") and tasked me to "image and inspect any hard drive used by Defendants in furtherance of their business in an effort to recover any relevant email communications or other relevant ESI from Defendants' email accounts and hard drives." (Order Appointing Special Master, Dkt. Doc. 26). The Court granted to me the necessary powers to proceed and ordered that the parties give me their full cooperation and afford me prompt access to any and all facilities, files, documents, media, systems, databases and personnel (including technical staff and vendors) which I deemed necessary to complete my duties.

I received the appointment order on May 30, 2014, whereupon I reviewed the operative pleadings, motions, affidavits and exhibits, and, on June 9, I furnished instructions to the parties respecting various matters, including the preservation of potentially relevant systems and media. I also posed three questions to the Defendants, viz.:

1. What electronic storage media did each Defendant use in furtherance of their business?

"Electronic storage media" includes hard drives, thumb drives (a/k/a "USB keys") and other solid state media, recordable optical media, magnetic tape, handheld device (e.g., phone or tablet), RAID arrays (including any NAS or SAN devices), e-mail accounts used after 1/1/2010 and Cloud (online) storage. It includes any media in your care or custody as well as any subject to your control, including any actual or contractual right of access.

"In furtherance of their business" should be read broadly to include devices that may have been incidentally used to store, transmit or receive business-related information or communications, now or after 2011.

In identifying such media, please endeavor to advise me as to, as feasible, its form, interface, capacity and time in service. For example, "an HP Pavilion Slimline Desktop serial number XYZ123 with a 1TB SATA hard drive used since May 2013" or "Jane Doe has maintained Gmail account JDoe1957 since approximately February 2010."

2. Who has custody of any physical electronic storage media identified above, and in what location(s)?

3. Are there any devices and/or storage media previously used in furtherance of the business that are believed to be wiped, missing, damaged or non-functional (e.g., "crashed")?

I convened a teleconference with the parties on June 11, 2014 wherein counsel for both sides were asked to describe their expectations with respect to the scope and purpose of the contemplated examination and acquaint me with the relevant events and communications, insofar as they could be anticipated. Rafael Villalpando, Jr. was on the call and advised that the only computing devices and storage devices used in the business consisted of a Dell desktop machine, his personal Dell laptop and a single thumb drive. There had been a Sony Vaio machine used at one time, but it had been formatted and its whereabouts were unknown. He assured me that there were no backup devices nor any other data storage devices or media other than the three noted.

Attorney Adam Chambers, representing Arco Iris, further responded on June 13, 2014 for the four Spanish-speaking brothers who are principals in the business. The relevant portions of Mr. Chambers' response are made Appendix A hereto.

Acquisition

On June 14, 2014, I travelled to the business premises of Arco Iris Ice Cream Company at 1435 Frio City Road in San Antonio. The premises are a pair of single-story structures containing retail space, storage areas, multiple factory/plant spaces and a small, windowless office. There I met Rafael Villalpando, Jr., who remained with me throughout the many hours I was working on the premises. Mr. Villalpando was courteous and solicitous to me at all times.¹

¹ On multiple occasions during the day, Mr. Villalpando sought to engage me in substantive discussions concerning the examination and sought to volunteer information concerning his actions with respect to the machines. Each time he did so, I stated, as politely as possible, that I could not discuss the case or my findings with him, and I could offer no advice whatsoever. I repeatedly advised him to address all such matters with Arco Iris' defense counsel and not with me.

When I requested that I be supplied with the devices and media used in the furtherance of the business, I was directed to the small office where the following devices were made available:

1. Dell Inspiron 560 desktop PC (service tag 9J5NYQ1), shipped by Dell in July 2011 and holding a 1 terabyte Western Digital WD10EALX 3.5" hard disk drive (S/N: WCATR7807292);
2. Dell Inspiron 1501 laptop PC (service tag 4GN6HD1), shipped by Dell in October 2007 and holding a balky 120GB Toshiba MK1237GSX 2.5" hard disk drive (S/N: 774ITJKIT); and,
3. Kingston Data Traveler 2GB USB thumb drive.

I photographed each device and set about forensically imaging all three. The one terabyte desktop drive and the 2GB thumb drive acquired and authenticated without difficulty within several hours; however, the laptop drive failed to yield an authenticable image while on site despite many hours of overall effort. Accordingly, and with Rafael Villalpando Jr.'s consent, I brought the laptop hard drive to my lab in Austin and successfully acquired its contents using a reverse imaging technique. I returned the drive to its owner by Federal Express.

Processing

The data collected was independently processed in two forensic processing and analysis platforms and, in each environment, the deduplicated item count numbered in excess of one million discrete items (files and folders). The volume snapshots were refined by, *e.g.*, a thorough search for orphaned file system data structures, carving by binary signature for potentially relevant deletions, signature verification against extensions, file hashing, extraction of metadata, thorough unpacking of compound and container files and file format specific and statistical encryption tests.

The volume snapshots were then searched using various keywords and Boolean queries; some suggested by the parties and others of my own choosing. The data was filtered for potentially relevant file types and manually reviewed for relevance in the focal interval. Closest attention was given to e-mail messaging, attachments and artifacts, as well as to assessing the nature and impact of the antifoensic activity identified. The data was assembled and reviewed by various analytic methods including, *inter alia*, timeline analysis, network and event mapping and domain and address listings.

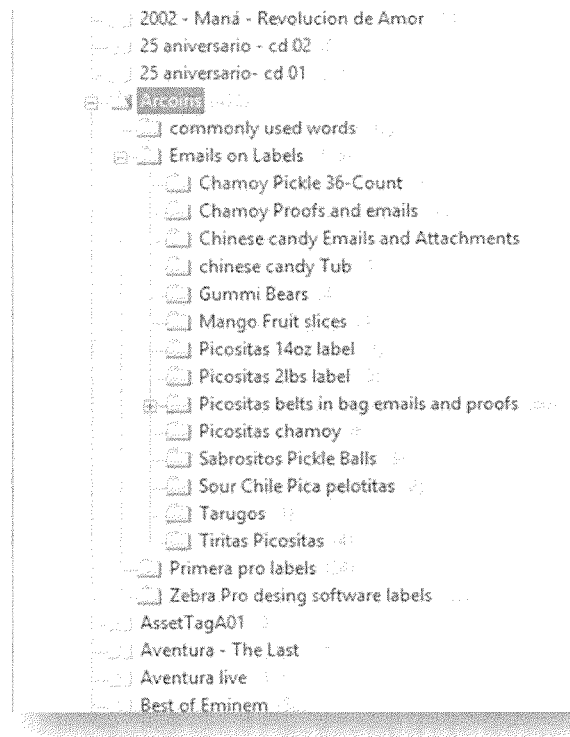
Examination and Analysis

During the phone conference with counsel, Rafael Villalpando, Jr, repeatedly assured me that all potentially relevant media had been disclosed.² I pressed rather hard on this issue and advised

² I asked Rafael Villalpando, Jr. and his counsel, "So, no other crashed or damaged, wiped, missing media?-devices, anything capable of storing electronic information than what's on the list provided to me? Am I missing anything?" Mr. Villalpando twice stated in response, "No, that should be it." He added, "No, I

all parties to the call that forensic analysis would likely reveal the attachment of undisclosed USB storage devices. Ultimately, examination of the desktop PC image did identify an undisclosed USB flash drive (serial number: EA25C5F7) that was connected to the desktop PC on May 28, 2014 at 08:10:37am. This date is one day following the Court's appointment and inspection order, and I anticipate this undisclosed device was used to install data destruction software on the desktop PC, as discussed below. Without production of the device, I cannot certify that it served as the source of the antifoensic application, CCleaner. To the extent that this thumb drive may hold relevant content and was not disclosed despite repeated inquiry and a court order for its production, I recommend that the Court further order it found, preserved and produced for examination. However, to produce it simply to establish spoliation is likely not necessary as there is ample evidence of the deployment and use of CCleaner without incurring the cost to obtain cumulative data

The Kingston Data Traveler thumb drive supplied (serial number 5B830D0002D6) proved to be something of a red herring in the analysis. It contained no content placed on same after September 30, 2013. Of the content seen on the thumb drive, only four files were accessed during 2014, all of these on June 10, 2014.³ The drive principally held deleted music files, along with a folder tree of information called "Arcoiris," containing material that is likely related to the issues in the case. See figure at right.⁴ This data was readily accessible; *i.e.*, it is active data requiring no forensic recovery. I recognized some of the files as containing information previously produced in



can't think of any other storage devices that we may have....The only ones I use are the ones I provided to you, that you have on the list."

³ The four files accessed were:

1. AM1 Wholesale, Inc.'s Motion for Partial Summary Judgment.docx
2. Arcoiris Gastos.xlsx
3. Customer list Arcoiris.xlsx
4. First Set of Requests for Production to Defendants ARCO IRIS Ice Cream and its General Partners..docx

⁴ Please note that the numbers alongside each folder do not correspond to discrete files or e-mail messages within each folder, but rather to files, folders and embedded objects. Multiple objects may comprise a single document.

discovery. On the thumb drive, these folders held the sole data referencing *"rafaelvillalpando@hotmail.com."*

Respecting the laptop machine, I noted the presence 16,238 files and folders deployed for the purpose of displacing (i.e., overwriting) potentially recoverable data. All of these were created on 5/27/14, with the data deletion and overwriting process begun at 2:46PM (-500UTC or Central time).

On the desktop machine, some 46,000 files and folders for the same purpose were created after 9:25am on May 28, 2014.

The contents of these 62,000+ files consisted exclusively of zeros. All have names composed of periods and the letter “Z.” (e.g., **ZZ.ZZ.ZZ.Z**). See figure at right. This naming convention is characteristic of an evidence elimination technique employed by the data hiding application, CCleaner by Piriform. These numerous files are created to overwrite deleted data, thus rendering it unrecoverable using digital forensic tools and techniques.

[illegible]

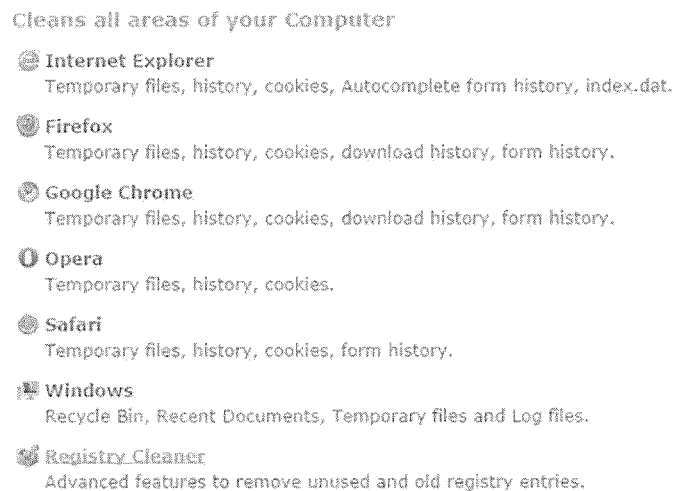
Spoliation

My opinion, based upon my analysis of the media, the configuration of CCleaner and my prior experience with its use, is that the installation and use of CCleaner demonstrates an intentional effort to shield electronic information from discovery and to decimate potentially relevant information, including the targeted destruction of Internet cache data. The forensic vestiges of web mail residing outside of an e-mail client collection tend to reside within the overwritten Internet cache. Thus, the information which the Court directed be examined in its order of May 27, 2014 was the very information purposefully eradicated from the Villalpando laptop and the Arco Iris desktop on the afternoon of May 27 and the morning of May 28, respectively.⁵

⁵ During the phone conference with counsel and Rafael Villalpando, Jr., I inquired if “privacy” applications like CCleaner had been run against the machines and Mr. Villalpando stated that he had used CCleaner and “run it about once a month.” The evidence on the machine was that the application was installed and first run on each machine *only after* the Court’s order. To be clear, the *setup program* for a 2008 version of CCleaner (ver. 2.14) was present on each machine, located in a backup folder on each machine; however, the program employed had not been installed or run prior to the Court’s order of May 27, 2014, nor prior to the Plaintiff’s motion precipitating my appointment. In fact, the version of the program

| Timeline | |
|----------------------|--|
| Date and Time (CDT) | Event |
| May 27, 2014 | Court appoints Special Master and orders acquisition and inspection of media "in an effort to recover relevant email communications and other relevant ESI." |
| May 27, 2014 12:32pm | CCleaner installed on LAPTOP PC |
| May 27, 2014 2:46pm | Data wiping software CCleaner is run on LAPTOP PC (wipe free space enabled) |
| May 28, 2014 8:10am | Generic thumb drive with serial number EA25C5F7 attached to DESKTOP PC |
| May 28, 2014 9:01am | CCleaner installed on DESKTOP PC |
| May 28, 2014 9:25am | Data wiping software CCleaner is run on DESKTOP PC |

CCleaner is a free application published by Piriform (<http://www.piriform.com/ccleaner>). Persons downloading CCleaner today would understand its capabilities, to include (per the Piriform website):

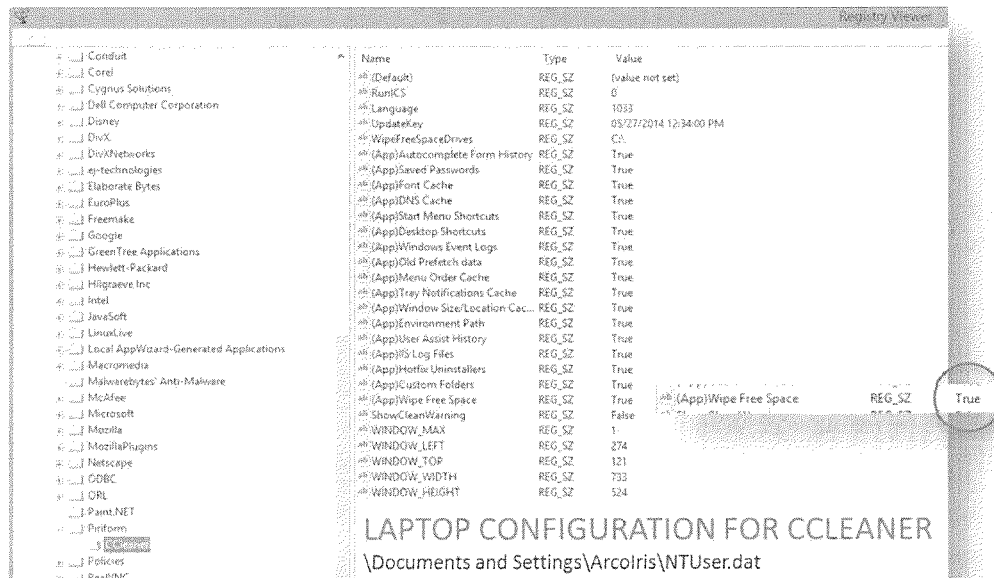


Evidence of Prejudice

The use of the CCleaner antifoensic tool adversely impacted the ability to recover active and deleted data from both machines. Based on the registry settings observed with respect to the installation of CCleaner on the laptop, a broad swath of forensically-significant active files was deleted and overwritten and remnant data residing within the unallocated clusters ("free space") of the drive were also overwritten. Notably, the setting to obliterate the free space of the drive

installed on both machines was a very recent version of the application (ver. 4.14), *which version was not available before May 22, 2014* (<https://www.piriform.com/ccleaner/version-history>).

is not the default setting on installation. Using the graphical user interface of the application, a user must affirmatively act to alter the default settings of the program to prompt a much more extensive disposal of data, and this was done with respect to the laptop machine. Proof of same is seen in the differing "True" and "False" values recorded in the system Registry for the configuration of "Wipe Free Space." (See figures below).

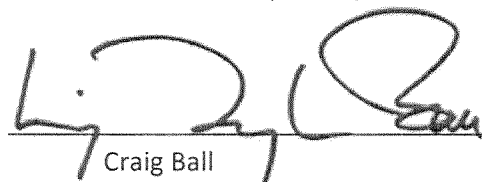


CCleaner was deployed less aggressively on the desktop PC in that the program was not configured to wipe free space at the time of my examination; notwithstanding, the regions of the file system targeted for obliteration on the desktop were those tending to hold much of the data that was the focus of the Court's order. These include, *inter alia*, Recycler contents, temp files, LNK files Internet cache, Internet history, cookies, recently typed URLs, index.dat files, MRUs and certain Windows log files. As noted, the overwriting of the free space on the laptop and of forensically-significant artifacts on both drives materially impaired the ability to resurrect other deleted data.

CCleaner is a tool of uneven efficacy in the eradication of forensically-significant artifacts. Accordingly, I was able to locate instances of some e-mail messaging exchanged during the years 2011 and 2012; however, none obtained in that interval bore on the matters at issue. (e.g., candy labelling and trade dress). I did not locate any relevant e-mail from the lost Hotmail account (identified to me as "RafaelVillalpando@hotmail.com") dated after August of 2011. That is, I saw nothing to belie the Defendants' claim that the Hotmail account was closed in August of 2012. In the face of an antifoensic application having been run, I am challenged to attribute the paucity of relevant material to its intentional destruction or to such information never having existed on the machine or elsewhere. The breadth and timing of the actions strongly suggest a purpose related to the Court's order, and the uncertainty of the extent of prejudice to the plaintiff is, of course, a consequence of intentional acts undertaken to destroy data in the 48 hours following the Court's order that it be secured.

By my signature below, I affirm that the foregoing is true and correct to the best of my knowledge and belief.

Respectfully submitted this 28th day of September, 2014,

A handwritten signature in black ink, appearing to read "Craig Ball", written over a horizontal line.

Craig Ball
Texas Bar No. 01632200
Craig D. Ball, P.C.
3723 Lost Creek Blvd.
Austin, Texas 78735
craig@ball.net

APPENDIX A

Attorney Adam Chambers, representing Arco Iris, supplied the following information to Craig Ball on June 13, 2014, responding on behalf of the four Spanish-speaking brothers who are principals in the business:

Rafael Villalpando, Sr.

Q1: Since the beginning of 2010, what are the computers that you own (including members of your household) or have access to?

A: The computer located at Arco Iris business is the only computer that I own or have access to, and there is no computer in my household.

Q2: Identify any email accounts to which you had access, or to which someone accessed for you such that you or someone for you sent or received emails?

A: Only the ArcoIris Hotmail and Ymail accounts.

Q3: Since the first quarter of 2010, please identify every cell phone, tablet or other device that you have used?

A: Since before 2010, I owned a Nokia phone. I do not know the model number or name of the phone. This phone was stolen while I was in Mexico in early 2013. I replaced the phone with an iPhone 5s, which I still have.

Q4: What happened to the Sony Vaio computer that used to be the business computer?

A: I am not sure, but I think that the computer was donated to the Salvation Army. I do not know whether the hard drive was wiped or any data deleted. I don't know how to do that.

Elias Villalpando

Q1: Since the beginning of 2010, what are the computers that you own (including members of your household) or have access to?

A: I purchased an HP Pavilion Desktop Model: RD01D850 computer for my children a few years ago, but that computer stopped working within the last year. I rarely used that computer for YouTube, or accessed it, because it was purchased for my children. The computer is still at my house. In 2013, I purchased my children a Toshiba Satellite C55t-A5102 Serial #: ZD243777Q. I did not use the Arcoiris computer. In 2012, I purchased a Tablet Kindle 5 (does not work) for the children.

Q2: Identify any email accounts to which you had access, or to which someone accessed for you such that you or someone for you sent or received emails?

A: I did not use email or have someone send or receive email on my behalf.

Q3: Since the first quarter of 2010, please identify every cell phone, tablet or other device that you have used?

A: From before 2010 until mid-2013, I owned a Cricket or T-Mobil Samsung phone with camera. I am not sure of the model of this phone. I still have this phone at home. In mid-2013, I switched to an Arcatel T-Mobil phone that I am using now.

Q4: What happened to the Sony Vaio computer that used to be the business computer?

A: I don't know.

Guillermo Villalpando

Q1: Since the beginning of 2010, what are the computers that you own (including members of your household) or have access to?

A: I purchased a laptop, a Dell Inspiron: 14z Service tag: 3917RS2, in Sep 2012 for my daughter, but I never used that computer or had access to it, because it was purchased for my daughter. The computer is still at my house. I did not use the Arcoiris computers.

Q2: Identify any email accounts to which you had access, or to which someone accessed for you such that you or someone for you sent or received emails?

A: I did not use email or have someone send or receive email on my behalf.

Q3: Since the first quarter of 2010, please identify every cell phone, tablet or other device that you have used?

A: From 2006 until sometime in 2011, I owned a Samsung phone with T-Mobil. I am not sure of the model of this phone other than it was a simple phone. This phone was discarded in 2011. After that, I owned a Cricket flip-phone that is a Tri-Band ZTE model A210 that I still use.

Q4: What happened to the Sony Vaio computer that used to be the business computer?

A: I don't know.

Raul Villalpando

Q1: Since the beginning of 2010, what are the computers that you own (including members of your household) or have access to?

A: I purchased a Desktop (Sony Vaio Model: PCV-2234) for my sons a few years ago, but I never used that computer or accessed it, because it was purchased for my sons. The computer is still at my house. I did not use the Arcolris computers, except I may have occasionally watched a You Tube video in the presence of my brothers or other family.

Q2: Identify any email accounts to which you had access, or to which someone accessed for you such that you or someone for you sent or received emails?

A: I did not use email or have someone send or receive email on my behalf.

Q3: Since the first quarter of 2010, please identify every cell phone, tablet or other device that you have used?

A: From 2008 to the present, I have owned a Samsung SCHR 430 flip-phone with a camera with Cricket.

Q4: What happened to the Sony Vaio computer that used to be the business computer?

A: I don't know.

Salvador Villalpando

Q1: Since the beginning of 2010, what are the computers that you own (including members of your household) or have access to?

A: My wife has a personal computer at the house, but I haven't ever used this computer. The Computer is a Gateway touch screen All-in-One. Additionally, we have a Dell All-in-One computer and a Samsung Galaxy Tablet in the house.

Q2: Identify any email accounts to which you had access, or to which someone accessed for you such that you or someone for you sent or received emails?

A: I did not use email or have someone send or receive email on my behalf.

Q3: Since the first quarter of 2010, please identify every cell phone, tablet or other device that you have used?

A: From 2010 to the beginning of this year, I had an AT&T flip phone. I discarded the flip-phone when I replaced it with a Samsung SGH1827 phone four or five months ago.

Q4: What happened to the Sony Vaio computer that used to be the business computer?

A: I don't know.

ATT.com email account and Rafael5911@terra.com

These accounts were used by Rafael Villalpando, Jr. as personal accounts, and we will provide all information necessary to access these accounts. There may have been incidental business communications on these accounts. The Rafael5911@terra.com account has not been accessed in quite some time, because he has forgotten the password.

Email addresses reserved but not used by the business

In conjunction with a redesign of the business website this March and April, I reserved email addresses for each of the principals of the business: The website was created by, and the email addresses issued by: AZENZ Marketing Solutions. I had not yet given the principals access to these email addresses, and they have not yet been accessed by any of them. These email addresses are:

rafaelv@arcoirisicecream.com

salvadorv@arcoirisicecream.com

eliasv@arcoirisicecream.com

raulv@arcoirisicecream.com

memov@arcoirisicecream.com